IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, LLC,
Plaintiff,

v. Civil Action No. 2:21-CV-00137 (EWH)

PALO ALTO NETWORKS, INC.,
Defendant.

MEMORANDUM OPINION AND ORDER

This matter comes before the Court for claim construction. Centripetal Networks, LLC ("Centripetal") brought this action against Palo Alto Networks, Inc. ("PAN") alleging infringement of five cybersecurity patents ("Asserted Patents").[1] The parties stipulated to the construction of six claim terms. Am. Joint Claim Construction Chart, ECF No. 419. The Court ADOPTS those constructions as listed in the stipulation. The parties dispute the construction of ten claim terms and have asked the Court to construe those terms.

Opening claim construction briefs were filed on July 14, 2023. Def.'s Opening Claim Construction Br. ("Def.'s Opening Br."), ECF No. 357; Pl.'s Opening Claim Construction Br. ("Pl.'s Opening Br."), ECF No. 359. Responsive briefs were filed on July 28, 2023. Def.'s Reply Claim Construction Br. ("Def.'s Resp. Br."), ECF No. 363; Pl.'s Responsive Claim Construction Br. ("Pl.'s Resp. Br."), ECF No. 366. On September 11, 2023, the Court held a *Markman* hearing. Tr. of Proceedings (Markman Hearing) ("Tr."), ECF No. 438. Subsequently, the Court ordered the parties to submit supplemental briefing. The parties submitted their supplemental briefs on October 2, 2023. Pl.'s Suppl. Claim Construction Br. (Pl.'s Suppl. Br.), ECF No. 445; Def.'s Suppl. Claim

[1] The Asserted Patents include U.S. Patent No. 10,567,437 (the "'437 Patent"), U.S. Patent No. 10,735,380 (the "'380 Patent"), U.S. Patent No. 10,659,573 (the "'573 Patent"), U.S. Patent No. 10,530,903 (the "'903 Patent"), and U.S. Patent No. 10,931,797 (the "'797 Patent").

Construction Br. ("Def.'s Suppl. Br."), ECF No. 448. Having considered the briefs, the exhibits attached thereto, the argument of counsel at the hearing, and applicable law, the Court now construes the disputed claim terms as set forth below.

I. LEGAL STANDARDS

Claim construction is the process of "determining the meaning and scope of the patent claims asserted to be infringed." *Markman v. Westview Instruments*, Inc., 52 F.3d 967, 976 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996). Construing patent claims is a question of law, although it may require subsidiary fact finding. *Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 324–26 (2015).

When engaging in claim construction, the Court must examine all the intrinsic evidence related to the claim terms. *Day Intern., Inc. v. Reeves Bros., Inc.*, 260 F.3d 1343, 1348 (Fed. Cir. 2001). Intrinsic evidence includes the claim language, specification, and prosecution history. *Interactive Gift Exp., Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1331–32 (Fed. Cir. 2001) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)) (describing the hierarchy of intrinsic evidence). Claim terms "are generally given their ordinary and customary meaning." *Vitronics Corp.*, 90 F.3d at 1582. "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art [("POSITA")] in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (citations omitted). The context of the term as it is used in the asserted claim "can be highly instructive." *Id.* at 1314. A disputed term's use in unasserted claims is also helpful in claim construction. *Id.* (citations omitted) ("Because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims.").

Patent claims must also be read in context of the specification. *Vitronics Corp.*, 90 F.3d at 1582. The specification may expressly define terms or define terms by implication. *Id.* (citing *Markman*, 52 F.3d at 979). Additionally, the specification, which "must be clear and complete enough to enable [a POSITA] to make and use it," is "always highly relevant" and in many cases "dispositive" in claim construction. *Id.*

The prosecution history, if it is in evidence, is also instructive. *Phillips*, 415 F.3d at 1317. The prosecution history consists of the "complete record of the proceedings before the [Patent and Trademark Office]," and includes *inter partes* review ("IPR") proceedings before the Patent Trial and Appeal Board ("PTAB"). *Id.* (citation omitted); *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1359–60 (Fed. Cir. 2017) (explaining that *inter partes* review proceedings are a part of the prosecution history). This record "provides evidence of how the [Patent and Trademark Office] and the inventor understood the patent" and can indicate "whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be." *Phillips*, 415 F.3d at 1317 (citation omitted). A prosecution disclaimer must be "both clear and unmistakable." *Aylus Networks*, 856 F.3d at 1359 (quoting *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003)).

If intrinsic evidence alone does not resolve the ambiguity of a disputed claim term, the Court may consider extrinsic evidence. *Vitronics Corp.*, 90 F.3d at 1583. Evidence such as technical dictionaries and treatises may assist the Court in understanding the underlying technology and may shed light on how a POSITA would understand claim terms. *Phillips*, 415 F.3d at 1317–18. Expert testimony may also assist the Court in claim construction; however, "conclusory, unsupported assertions by experts as to the definition of a claim term are not useful" and the Court "should discount any expert testimony that is clearly at odds" with the intrinsic evidence. *Id.* at 1318 (internal quotation marks and citations omitted).

II. CLAIM CONSTRUCTION

The ten disputed claim terms are from five Asserted Patents, and three patent families, which the parties generally categorize as follows:

The Correlation Patents or Ahn Patents ('903, '573, '797 Patents);
The Exfiltration Patent or Moore Patent ('380 Patent); and
The Packet Security Gateway or Rogers Patent ('437 Patent).

All of the Asserted Patents relate to network security, specifically systems and methods for evaluating packets of information travelling through a network. The Correlation Patents "generally disclose systems and methods for 'correlating packets in communication networks.'" Pl.'s Opening Br. at 2, ECF No. 359 (citing '573 Patent at Title). The Exfiltration Patent "relate[s] to filtering network data transfers" to prevent the exfiltration of data. '380 Patent at 1:31–34, 1:65–66. And finally, the Packet Security Gateway Patent discloses systems and methods for protecting a secured network by placing packet security gateways at the boundary between networks which filter packets leaving and entering the secured network. '437 Patent at 5:30–37, 16:59–17:3, fig. 7. The three patent families share some of the same disputed claim terms. Having reviewed the intrinsic and relevant extrinsic evidence, the Court will construe the ten disputed claim terms as follows:

A. "Configured" / "Configure to" / "Configured to"

The term "configured," or its variations, appear in claim 10 of the '903 Patent, claims 1 and 9 of the '573 Patent, claims 1, 12, and 17 of the '797 Patent, and claim 8 of the '437 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
"capable of configuring"	Requires pre-existing programming of hardware and software to perform the cited functionality without modification

Centripetal argues that "configured" should be construed to include "capable of," whereas PAN argues that "configured" should be interpreted to mean that the functionality cited in the claim is pre-existing and does not require modification to occur.

The International Trade Commission ("ITC") handled a nearly identical dispute regarding a related patent[2] in an investigation initiated by Centripetal against Keysight Technologies, Inc. *In the Matter of Certain Computer Network Security Equipment and Systems, Related Software, Components thereof, and Products Containing Same*, USITC Inv. No. 337-TA-1314, Order No. 37, 2023 WL 2237698, at *7–15 (Feb. 22, 2023) (Markman Claim Construction). During claim construction in that matter, Centripetal argued that "configured to" should include "capable of performing the functionality claimed." *Id.* at *7. The ITC disagreed, explaining that "configured to" is a term of art used in patents across many fields and that "'[c]onfigured to' is interpreted more narrowly than 'capable of,'" absent language in the claims or specification that indicates otherwise. *Id.* at *9 (citing *Radware Ltd. v. A10 Networks, Inc.*, No. C-13-02024-RMW, 2014 WL 1572644, at *12 (N.D. Cal. Apr. 18, 2014)). After examining the language of the patent at issue and its specification, the ITC concluded that the claims did not include any "capable of" language and accordingly found that "the term 'configured to' is given its plain and ordinary meaning, i.e., requires pre-existing programming of hardware and software to perform the cited functionality

[2] At issue in the ITC proceeding is U.S. Patent No. 9,264,370 from the Ahn family of patents.

without modification." *Id.* at *9–15. PAN proposes the construction adopted by the ITC in that proceeding.

Like the claims before the ITC, the claim language at issue here does not support a "capable of" interpretation. For example, claim 9 of the '573 Patent describes "[a] computing device comprising:"

> at least one processor; and
>
> memory comprising instructions that, when executed by the at least one processor, cause the computing device to: . . .
>
> > generate, based on the correlating, one or more rules *configured to* identify packets received from the host located in the first network; and
> >
> > provision a packet-filtering device with the one or more rules *configured to* identify packets received from the host located in the first network.

'573 Patent at 17:1–5, 29–34 (emphasis added). As is evident, the words of the claim recite "configured to" rather than "capable of."

The context of the claims also supports the "configured to" interpretation. Claim 9, like the patent considered by the ITC, requires the computing system to undertake a series of interrelated actions. *See In the Matter of Certain Computer Network Security Equipment and Systems, Related Software, Components thereof, and Products Containing Same*, 2023 WL 2237698, at *13. Specifically, claim 9 instructs that the computing device will first "identify a plurality of packets" and "generate . . . log entries corresponding" to the packets received, then identify a plurality of encrypted packets, and generate a second set of log entries. '573 Patent at 17:6–16. The log entries are used in the correlation step, which in turn is used to generate one or more rules "configured to identify packets received from the host." *Id.* at 17:17–31. The instructions of the claim—to identify packets, generate log entries, correlate, generate rules, and provision those rules—"all rely on each other" in causing the computing device to operate as cited. *In the Matter of Certain Computer Network Security Equipment and Systems, Related Software, Components thereof, and Products Containing Same*, 2023 WL 2237698, at *13. Like the patent considered by the ITC, "the rules are necessarily configured/programmed as cited in [claim 9] as required by the term as it appears in the context of the claim as a whole." *Id.* Thus, the system must not merely be "capable of" being configured, but in fact be configured, based on the correlating, to generate rules to identify packets. The language of the other relevant patent claims is similar and also does not support a "capable of" interpretation. *See* Patent '437 at 22:66–23:4; Patent '903 at 16:59–64; Patent '797 at 15:45–47. Because the patent claims do not include conditional language that supports a "capable of" interpretation, the Court rejects Centripetal's construction in favor of the ITC construction. *See SIPCO, LLC v. Abb, Inc*, No. 6:11–CV–0048, 2012 WL 3112302, at *10–11 (E.D. Tex. July 30, 2012).

Centripetal raises two concerns with the ITC construction. First, Centripetal takes issue with the inclusion of "pre-existing" and "without modification." Centripetal argues that "pre-existing" and "without modification" restrict the claim such that it does not accurately reflect that the rules are being generated after correlation or some other process. Pl.'s Opening Br. at 6, ECF No. 359 ("The rules cannot be generated until the correlation occurs, and thus the generated rules would not pre-exist via the programming of hardware and software without modification . . . ."). The Court disagrees with Centripetal's assertion that the ITC construction is inconsistent with the claim language. A POSITA[3] reading the claim language in the context in

[3] Centripetal and PAN proposed two slightly different definitions of a POSITA; however, the parties agree that the differences are immaterial for the purposes of claim construction. Tr. at 29:10–30:5; 42:24–43:1, ECF No. 438. The Court concurs and does not resolve any of the claims based on the apparent differences in definitions.

which it appears would understand that the rules are being generated based on the correlating. *See, e.g.*, ’573 Patent at 15:49–55 (“*[G]enerating*, by the computing system and *based on the correlating*, one or more rules configured to identify packets . . . .” (emphasis added)). However, the claim language is also equally clear that the correlating, and the subsequent generating of the rules, occurs when the instructions are executed, without modification to the underlying software or hardware. *See id.* at 17:1–5 (“A computing device comprising: at least one processor; and memory comprising instructions that, when executed by the at least one processor, cause the computing device to: . . .”). PAN’s proposed construction allows for the generating of rules while maintaining that the underlying hardware and software are already configured in a way that allows that generating to occur.

Second, Centripetal contends that PAN’s proposed construction is improper because it requires “programming of hardware and software,” while the specification makes clear either can be used. Pl.’s Opening Br. at 7, ECF No. 359. The Court agrees that the specification of the ’437 Patent contemplates “an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or [a combination].” ’437 Patent at 20:37–45. However, all the Asserted Claims appear to include both software and hardware components. *See, e.g.*, ’437 Patent at 22:25–28 (“A system comprising: at least one processor; and memory storing instructions . . . .); ’573 Patent at 15:25–55 (referencing a “computing system”); ’797 Patent at 17:48–50 (“One or more non-transitory computer-readable media comprising instructions that, when executed by one or more processors of a computing device . . . .”). Centripetal has not identified any claim language to the contrary.

Accordingly, the Court adopts PAN’s construction.

Court's Construction
Plain and ordinary meaning, i.e., requires pre-existing programming of hardware and software to perform the cited functionality without modification to the hardware or software

B. "Network Exfiltration Methods"[4]

The term "network exfiltration methods" appears in claims 16 and 25 of the '380 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
Plain and ordinary meaning	"the unauthorized transfer of data from a computer by malware or a malicious actor"

Centripetal argues that the term "exfiltration" is readily understood by a POSITA and requires no construction. Pl.'s Opening Br. at 19, ECF No. 359. Centripetal also contends, however, that the specification explains that exfiltration can happen in a number of different contexts, such as "stealing sensitive data or credentials via the Internet." *Id.* (citing '343 Patent at 1:28–30). And while Centripetal acknowledges that exfiltrations "may be unauthorized or done 'by malware or a malicious actor,'" it notes "that is not true in every instance," and may occur through a user's inadvertent or accidental action. *Id.* at 20. PAN contends that the intrinsic record and Centripetal's own statements make clear that exfiltrations describe only unauthorized actions. Def.'s Resp. Br. at 22–23, ECF No. 363. The parties' disagreement thus turns on the issue of

[4] The parties initially requested that the Court also construe the terms "Exfiltration," "Exfiltration Operation," and "Network Exfiltration" which appear in the '343 Patent. Accordingly, the parties' briefing and proposed constructions focused on defining the root word "exfiltration." The parties subsequently agreed to a partial stay of the case as it relates to the '343 Patent. ECF No. 399. Although the relevant claims of the '380 Patent just contain the term "network exfiltration methods," the Court only finds it necessary to construe the root word "exfiltration."

whether "network exfiltration methods" refers to exfiltrations which are unauthorized and conducted by either malware or a malicious actor or also include inadvertent or accidental actions.

The claim language itself does not shed additional light on the term, requiring that an operator be applied to certain packets "based on a determination that the identified data transfer request field indicates one or more network exfiltration methods." *See* '380 Patent at 13:59–14:2. Nevertheless, the specification and Centripetal's statements to the PTAB support PAN's construction.

The specification of the '380 Patent describes exfiltrations as a "category of cyber attack" which includes "stealing sensitive data or credentials via the Internet." *Id.* at 1:31–32. It then goes on to list reasons why preventing exfiltrations is difficult. *Id.* at 1:32–54. Among other reasons, the specification states that preventing exfiltration is difficult because "human users often knowingly or unknowingly engage in network activities that are vulnerable to attack." *Id.* at 1:41–43. Centripetal argues that this example is describing a type of exfiltration that is inadvertent and non-malicious. Pl.'s Opening Br. at 20, ECF No. 359. Centripetal's reliance on this language is misplaced, as its interpretation misconstrues the specification language. The specification does not characterize the human user's actions as exfiltration, it simply notes that the user's actions may make exfiltration more likely (i.e. more "vulnerable to attack"). Stated differently, the exfiltration is effectuated by someone other than the human user (i.e. a hacker), although it may have been facilitated by the inadvertent acts of the human user. Centripetal's position would significantly broaden the claims to include non-intentional acts conducted by benign actors as "exfiltrations." The specification does not support such an interpretation.

Further, Centripetal's statements to the PTAB also align with PAN's construction. The inventor of the '380 Patent explained exfiltrations to the PTAB when Centripetal was defending a related patent:[5]

> Centripetal's products prevent a category of cyber-attack known as data exfiltration. Data exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer. For example, a cyber-criminal might steal data such as usernames/passwords, personal information, financial data, or corporate trade secrets, and exfiltrate that data out from a computer or network and into their possession.

In re Ex Parte *Reexamination of U.S. Patent No. 9,686,193*, Control No. 90/014476, Moore Decl. ¶ 6 (Jan. 25, 2020), ECF No. 358-19. Further, when defending the '380 Patent, Centripetal explained that "[e]xfiltration refers to cybersecurity attacks that hijack a computer on a network in an attempt to send information to malicious actors" and includes "information leaving a network in an unauthorized manner." *Palo Alto Networks, Inc. v. Centripetal Networks Inc.*, IPR2021-01270, Paper 7, Patent Owner's Prelim. Resp. at 44 (P.T.A.B. Oct. 28, 2021). While these statements may not rise to the level of a disclaimer, they do assist the Court in determining how a POSITA would understand the term in the context of the patent. *See AstraZeneca AB v. Mylan Pharms. Inc.*, 19 F.4th 1325, 1335 (Fed. Cir. 2021) ("[E]ven in the absence of a clear and unmistakable disavowal, . . . the prosecution history can be evaluated to determine how a person of ordinary skill would understand a given claim term.").

Accordingly, the Court adopts PAN's construction.

Court's Construction
"the unauthorized transfer of data from a computer by malware or a malicious actor"

[5] The patent at issue before the PTAB was U.S. Patent No. 9,686,193 the grandparent patent of the '380 Patent.

C. "Responsive to [the correlating]" / "Based on [the determined correlation]"[6]

The third set of disputed terms appear in the Correlation Patents. "Responsive to [the correlating]" appears in claims 1 and 9 of the '573 Patent and in claim 10 of the '903 Patent, while the term "based on [the determined correlation]" appears in claims 1, 12, and 17 of the '797 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
Plain and ordinary meaning	"in reaction to"

To understand the dispute between the parties, it is necessary to discuss the context in which the disputed terms appear. Generally, each claim requires certain steps. For example, claim 1 of the '573 Patent discloses a method requiring the computing system to: (1) "identify[]" a group of packets received by the network device, (2) "generat[e]" log entries corresponding to those packets, (3) "identify[]" a group of encrypted packets transmitted by the network device, (4) "generat[e]" log entries corresponding to those packets, and then:

> correlat[e] . . . based on the first plurality of log entries . . . and the second plurality of log entries . . . the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device; and
>
> *responsive to the correlating* . . . :
>
> > generat[e], by the computing system and *based on the correlating*, one or more rules configured to identify packets received from the host located in the first network; and
> >
> > provision[] a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network.

'573 Patent at 15:25–55.

[6] Although Centripetal presented these two terms separately, the Court will address them together.

Centripetal argues that the plain and ordinary meaning is apparent from the context of the claims, "namely, that the 'generating' and 'provisioning' steps are done in response to the correlating." Pl.'s Opening Br. at 16, ECF No. 359. PAN largely agrees, arguing that each of the asserted claims "recite[] performing steps (e.g., 'generating,' 'provisioning,' 'transmitting') 'based on' or 'responsive to' 'the correlating' recited earlier in the claim." Def.'s Opening Br. at 22, ECF No. 357 (emphasis omitted). But PAN seeks to define both "responsive to" and "based on" to mean "in reaction to." *Id.* Although these terms may appear to be synonymous with each other, PAN promotes its construction to enforce the idea that the correlating is *the impetus*, rather than *an impetus* (i.e. one of many), for the remedial steps described in the relevant claims. Def.'s Resp. Brief at 26, ECF No. 363. The dispute then, is not the particular word used (responsive to, based on, or in reaction to), but whether the claims permit something other than the correlation to cause the remedial steps to be performed.

The claim language and context, as well as Centripetal's statements to the PTAB when defending the '903 Patent, indicate that the correlating is *the impetus* for the remedial action. Claim 9 of the '573 Patent provides that "*responsive to the correlating*," the computing device must "generate, *based on the correlating*, one or more rules configured to identify packets received from the host located in the first network." '573 Patent at 17:25–31 (emphasis added). The language is clear that the generating of the rules is directly responsive to and based on the correlating. Relevant claims of the '903 Patent and the '797 Patent similarly indicate that the remedial action is caused by the correlating and do not contain language indicating that the action is a result of other causes. *See* '903 Patent at 17:19–21 ("[R]esponsive to the correlating: generate an indication of the first host; and transmit the vindication of the first host."); '797 Patent at 18:11–16 ("[D]etermine a correlation based on correlating the first plurality of packets and the second plurality of packets;

generate, based on the determined correlation, one or more rules configured to identify packets received from the first host . . . .”).

This interpretation is confirmed by Centripetal’s statements to the PTAB defending the patentability of the ’903 Patent. When distinguishing the ’903 Patent from the prior art, Centripetal stated:

> . . . [T]he ’903 Patent’s impetus for implementing remedial steps (e.g., generating an indication of a host and transmitting an indication) is done responsive to the correlating. That is, the remedial steps are in reaction to the correlating of packets. In contrast, Paxton’s and Sutton’s impetus for identifying nodes is the detection of malicious activity.

Palo Alto Networks, Inc. v. Centripetal Networks, Inc., IPR2021-01150, Paper 19, Patent Owner’s Resp. at 6 (P.T.A.B. May 18, 2022), ECF No. 358-21 (internal quotation marks and citations omitted). Centripetal goes on to explain that the plain and ordinary meaning of the term “responsive to” in the claim language “conveys to a POSITA that the remedial ‘generating’ and ‘transmitting’ steps must be performed in reaction to ‘correlating . . . at least a portion of the plurality of first packets and at least a portion of the plurality of second packets.’” *Id.* at 13–14 (internal citations omitted). Likewise, Centripetal maintained that the specification reinforces this interpretation. *See id.* at 15 (describing the specification and concluding “[t]he correlation of packets *thus triggers* the generating and transmission of an indication of a host” (emphasis added)). Centripetal’s statements to the PTAB further confirm for the Court that a POSITA would understand the claim language and the specification to support the construction that correlating is the impetus for the remedial action. *See AstraZeneca AB*, 19 F.4th at 1335.

However, the Court does not adopt PAN’s proposed “in reaction to” construction. That construction would not offer additional clarity beyond what “responsive to” or “based on” already provide. Instead, the Court finds that a POSITA would understand the plain and ordinary meaning of "responsive to" and "based on"—in the context which they appear—to mean that correlating is the impetus for the remedial action.

Court's Construction
Plain and ordinary meaning in the context which it appears, i.e. the correlating or the determined correlation is the impetus for the remedial steps

D. "Header region of the identified at least one application packet"

The term "header region of the identified at least one application packet" appears in claim 16 of the '380 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction[7]
Plain and ordinary meaning	"application layer header of the identified at least one application packet"

Helpful to understanding this dispute is the OSI reference model cited by both parties as extrinsic evidence. Villasenor Decl. ¶ 16, ECF No. 449-2 (citing Deon Reynders & Edwin Wright, *Practical TCP/IP and Ethernet Networking* (2003) ("Reynders")); *OSI Model*, TheNetworkSeal, https://thenetworkseal.wordpress.com/stp/network/, ECF No. 360-18. The OSI model (and similar models such as the TCP/IP model) set forth a layered structure representing the protocol for communicating information across networks. The purpose of "abstracting functions into different layers" is to allow "a specific protocol [to] focus on the functions of that layer without impacting other layers." Villasenor Decl. ¶ 16, ECF No. 449-2 (citing Reynders). In the OSI model, the layers include the application layer, presentation layer, session layer, transport layer, network layer, data

[7] PAN previously proposed "area of the packet header of the identified at least one application packet" for this term. Def.'s Opening Br. at 19, ECF No. 357. PAN amended its construction "to make clear the relevant header is the application layer header." Def.'s Suppl. Br. at 1, n.1, ECF No. 448.

link layer, and physical layer. Reynders at 23, ECF No. 358-17. As a data packet travels through these layers, each performs a particular function, adds header information to the packet, and passes the packet to the next layer for processing. *Id.* For packets carrying information associated with a particular software application, this process begins at the topmost layer, which is the application layer. This is illustrated below:

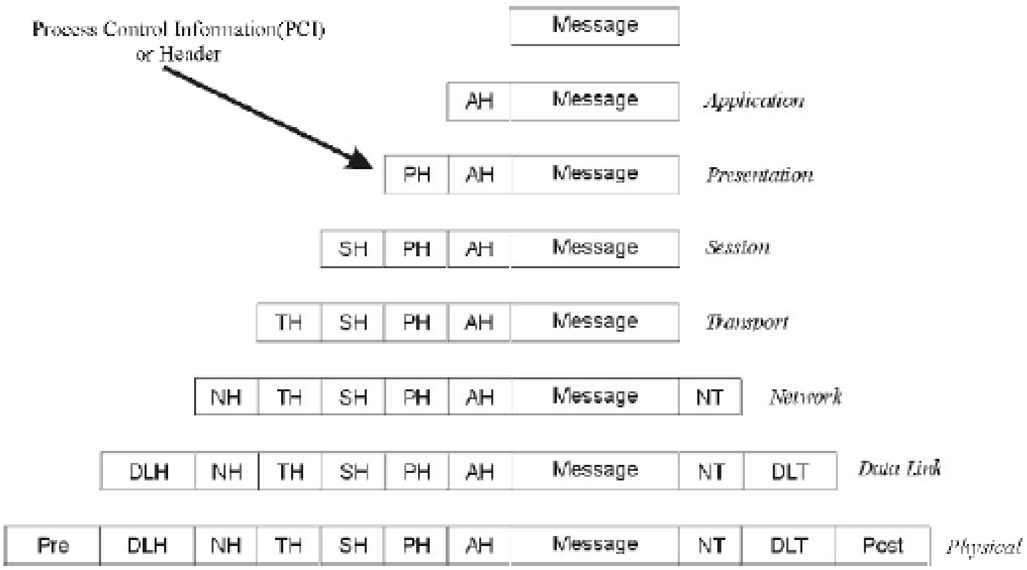
Process Control Information(PCI) or Header
Message
AH Message Application
PH AH Message Presentation
SH PH AH Message Session
TH SH PH AH Message Transport
NH TH SH PH AH Message NT Network
DLH NH TH SH PH AH Message NT DLT Data Link
Pre DLH NH TH SH PH AH Message NT DLT Post Physical

Figure 2.10
OSI message passing

Reynders, ECF No. 358-17; *see also OSI Model*, TheNetworkSeal, https://thenetworkseal.wordpress.com/stp/network/, ECF No. 360-18.

The disputed claim requires that a field within the "header region of the identified at least one application packet" be identified. The parties dispute which layer of the model is involved at this step, as well as what information (e.g. a particular header, data, or combination of both) is referenced. PAN argues that the language is referring to the header information generated at the application layer (listed above as "AH," and referred to here as "application layer header"). Def.'s Opening Br. at 19, ECF No. 357; Tr. at 86:10–22, ECF No. 438. Centripetal argues that "header region" should be understood more broadly. Centripetal contends that "the claim does not prohibit other data from other layers being considered in addition to the header of the application packet, such as the port information from a transport-layer packet, which may also contain information about the application." Pl.'s Suppl. Br. at 3–4, ECF No. 445 (citing Tr. at 68:22–69:4). Centripetal also argues that the claim language does not prohibit the evaluation of the packet's payload in conjunction with the "header region" because "the header region can describe the type of data contained in the payload." *Id.* at 5.

The claim language, specification, and extrinsic evidence align with PAN's construction. In the relevant portion, claim 16 of the '380 Patent explains that, when executed, the instructions cause the packet security gateway to: First, "receive a plurality of outbound in-transit packets departing the protected network" and "determine, based on one or more packet-filtering rules, that the first destination comprises a destination outside of the protected network." '380 Patent at 13:43–49. Second, it (1) "identif[ies] . . . at least one application packet contained in the first packets," (2) "determine[s] that the at least one application packet is associated with a data transfer protocol associated with one or more packet-filtering rules," (3) "identif[ies] *a data transfer request field within a header region of the identified at least one application packet*," (4) "determine[s] whether a value of the identified data transfer request field indicates that the data transfer protocol comprises one or more network exfiltration methods," and (5) applies an operator "based on a determination that the identified data transfer request field indicates one or more network exfiltration methods," which drops those packets. *Id.* at 13:50–14:2 (emphasis added). Importantly here, the disputed claim term appears in the second stage of actions.

The specification provides further context:

> The filtering process described herein may be viewed as having two (2) stages: A first stage in which the '5-tuple' of IP packet header field values and transport

> protocol (e.g., TC, UDP, etc.) packet header field values may be filtered; and, a second stage in which application packet header field values may be filtered (e.g. by applying operator logic . . .).

’380 Patent at 8:42–48; *see also id.* at 2:43–49. The first stage expressly contemplates looking at information contained in transport or network layer. *See What is a Packet? Network Packet Definition*, Cloudflare, https://www.cloudflare.com/learning/network-layer/what-is-a-packet/, ECF No. 446-2 (explaining that “IP (internet Protocol) is a network layer protocol”); *see also* Villasenor Decl. ¶ 23, ECF No. 449-2. To the extent that Centripetal argues that the first stage of the patent claim looks at network layer information, it is correct. However, the disputed term refers to what occurs in the second stage. At the second stage, the operator logic that is applied refers to “application-layer protocols,” such as the Hypertext Transfer Protocol (“HTTP”). *See, e.g.*, ’380 Patent at 7:13–16 (“. . . [A]n HTTP-EXFIL operator may allow HTTP packets containing a GET method, but may block HTTP packets containing other HTTP methods (e.g., PUT, POST, CONNECT, etc.).”). The HTTP protocol is carried out at the application layer. *See* Andrew S. Tanenbaum & David J. Wetherall, *Computer Networks* 45 (5th ed. 2011), ECF No. 358-15; *TCP/IP Model*, GeeksforGeeks, https://www.geeksforgeeks.org/tcp-ip-model/, ECF No. 446-1. Similarly, the abstract references first “packet header field values” and a “further determination” related to the “application header field values.” ’380 Patent at Abstract. Accordingly, the Court understands “header region of the identified at least one application packet” to refer to the application layer header.[8]

[8] This understanding is further supported by Centripetal’s statements to the PTAB when defending U.S. Patent No. 9,124,552, a parent patent of the ’380 Patent. In that matter, Centripetal described a two-stage process similar to the process described above, explaining that at the second step the applied operator specifies application layer packet header values. *See Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2018-01436, Paper 18, Patent Owner’s Resp. at 49 (P.T.A.B. Jul. 30, 2019) (“. . . [F]irst ensuring that the packet meets specified packet header criteria and then, if

Centripetal's arguments to the contrary are not persuasive. First, Centripetal contends that the "header region of the . . . application packet" can refer to "data from other layers . . . in addition to the header of the application packet" because data from those other layers may contain "information about the application." Pl.'s Suppl. Br. at 4, ECF No. 445. Centripetal notes that "port information from a transport-layer packet" may contain application-related information and therefore is part of the application packet's header region. *Id.* However, the claim requires the packet security gateway to "*identify a data transfer request field*" within the "header region of the . . . application packet," '380 Patent at 13:57–58 (emphasis added), and Centripetal does not contend that this field can be identified using data from layers other than the application layer. Centripetal's second argument is also inapposite. Centripetal insists that the claim language does not prevent an analysis of the packet's payload as well as the "header region" because "the header region can describe the type of data contained in the payload." Pl.'s Suppl. Br. at 5, ECF No. 445 (internal citation omitted). However, while the header region may describe data contained in the payload, the claim language explicitly references identifying a field value in the header and not the payload, *see* '380 Patent at 13:50–14:2, and the specification likewise references evaluating information contained within the headers, *see, e.g.*, *id.* at 7:13–26; 8:42–55. Accordingly, the patent does not contain any support for Centripetal's contention.

For these reasons, the Court adopts the PAN's proposed construction.

Court's Construction
"application layer header of the identified at least one application packet"

the packet header criteria is met, applying an operator that specifies *application-layer-packet header values* for which packets should be blocked." (original emphasis omitted) (emphasis added)).

E. "Malicious network traffic"

The term "malicious network traffic" appears in claims 1 and 8 of the '437 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
Plain and ordinary meaning	"network traffic intended to do harm"

The '437 Patent, which is titled "Methods and Systems for Protecting a Secured Network," involves the use of "packet security gateways" through which packets may pass. The term "malicious network traffic" appears in relation to packet filtering rules. For example, claim 8 of the '437 Patent provides that "each packet filtering rule comprises at least one packet matching criterion associated with *malicious network traffic* and a corresponding packet transformation function." '437 Patent at 22:36–39 (emphasis added). The dispute centers on whether the term "malicious," which is not defined in the claim language or in the specification, implies that the network traffic intends to do harm. The Court finds that the intrinsic and extrinsic evidence does not support such a limitation and, accordingly, rejects PAN's proposed construction.

In support of its argument that "malicious" requires an intent to do harm, PAN cites to Centripetal's response defending the patentability of a related patent[9] in which Centripetal stated that "[a] POSITA understands that malicious program code is a synonym for 'malware,' i.e. 'a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.'" *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01157, Paper 18, Patent Owner's Resp. at 28 (P.T.A.B. Jun. 7, 2022), ECF No. 358-13 (internal citation omitted). Centripetal's

[9] The patent at issue before the PTAB was U.S. Patent No. 10,749,906 from the Rogers family of patents.

statement, in context, provides an example of malicious program code, rather than a definition of the term malicious. Additionally, the extrinsic evidence, discussed below, confirms that a POSITA's understanding of the term does not require the intent to cause harm.

In support of its interpretation, PAN relies on the ordinary dictionary definition of "malicious." *See* Def.'s Opening Br. at 14, ECF No. 357 (citing the Oxford and Merriam-Webster dictionaries). While such general-usage dictionaries are helpful in certain contexts, they are unhelpful here where "malicious" is a technical term of art in the field of cybersecurity. *See Phillips*, 415 F.3d at 1314, 1318, 1321–22 (discussing the appropriate use of dictionaries in claim construction). More on point is the "malicious code" definition provided by the Cybersecurity and Infrastructure Security Agency ("CISA") which Centripetal relied on in IPR proceedings. *See Palo Alto Networks Inc. v. Centripetal Networks Inc.*, IPR2021-01157, Ex. 2034 (P.T.A.B. June 7, 2022). CISA describes malicious code as "unwanted files or programs that can cause harm to a computer or compromise data stored on a computer." *Id.* This definition is consistent with the technical dictionary relied on by PAN, which focuses on the harm to the system. *See* Microsoft Computer Dictionary 326 (5th ed. 2002), ECF No. 358-12 (defining "malicious mobile code" as "[a] virus or other destructive program that takes advantage of security weaknesses in wireless transmission systems"). Both definitions make clear that the construction proposed by PAN misconstrues the character of the traffic by focusing on the intent of the sender.[10]

The Court finds that "intended to do harm" is not supported by the claim language, specification, or extrinsic evidence, and is narrower than how a POSITA would understand the term "malicious network traffic" in the context of the patent. *See* Goodrich Decl. ¶ 38, ECF No.

[10] The Court's interpretation here is consistent with its interpretation of the term "Network Exfiltration Methods," which focuses on the unauthorized nature of the transfer, rather than the intent of the transferor.

361. Accordingly, the Court rejects PAN's proposed construction and adopts the plain and ordinary meaning of the term.

Court's Construction
Plain and ordinary meaning

F. "Packets"

The term "packets" appears in all five Asserted Patents. In fact, it is a central term in each patent, as each of the patents describe various methods and systems for evaluating packets of information travelling through a network. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
Plain and ordinary meaning in the context of the claim in which the term appears	"data units for transmission over a network that each include a header and payload, where the payload may be empty"

In previous related litigation, the Court described a "packet" in reference to related patents[11] to be "akin to a virtual box of information." *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, No. 2:18-cv-94, 2020 WL 863976 at *5 (E.D. Va. Feb. 20, 2020). Although the Court recognized this generic description, it also observed that the term could be used in different contexts, for example the term could refer to packets at a particular layer of the OSI model. *Id.* at *5–6. The Court found that "the patents themselves contemplate 'packets' at other layers." *Id.* (providing as an example, the '193 Patent (the grandparent patent of the '380 Patent) which references an "HTTP packet"). Accordingly, the Court construed the term packets to have its "plain and ordinary meaning, which will require reference to the context of the specific claim at issue." *Id.* at *6.

[11] The patents at issue in *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, included U.S. Patent No. 9,560,176, the parent patent of the '903 Patent; U.S. Patent No. 9,686,193 (the "'193 Patent"), the grandparent patent of the '380 Patent; and U.S. Patent No.. 9,137,205, the great-grandparent patent of the '437 Patent, among others.

The dispute here is related. Although the parties initially appeared to diverge significantly over the definition of a packet,[12] at the claim construction hearing both parties agreed that a packet is "data units for transmission over a network." Tr. at 98:2–3, 105:17–24, ECF No. 438; Def.'s Resp. Br. at 23, ECF No. 363. The parties disagree however, regarding whether "data units for transmission over a network" must include a header or a payload, or both.

The Asserted Patents themselves reference numerous types of packets, for example, application packets,[13] IP packets, "IP packets containing one or more TCP packets," "application-level HTTP packet," "TCP packets," and "encrypted packets."[14] Additionally, the term packets appears in a variety of different contexts across the Asserted Patents that reference different ways in which a packet may be received, distributed, or examined. For example, the '903 Patent references packets "received by a network device," '903 Patent at Abstract; the '380 Patent references the receipt of "outbound in-transit packets departing the protected network" and applies operators to those packets causing them to be dropped, '380 Patent at 13:43–46, 13:64–14:2; and

[12] Centripetal originally argued that "packets" may refer to a "log of packets, an application packet, or another type of data structure based on the context." Pl.'s Opening Br. at 11, ECF No. 359. At the claim construction hearing, Centripetal conceded that a packet does not refer to a log of packets and clarified that "another type of data structure" is simply a "data unit for transmission over a network." Tr. at 96:10–20; 105:17–24, ECF No. 438.

[13] Although the parties previously agreed that "application packet" be given its plain and ordinary meaning, their briefing suggests there is disagreement as to the meaning of this term as well. *See* Parties' Agreed upon Constructions, ECF 419-1; Def.'s Suppl. Br. at 2–3, ECF No. 448 ("[T]he '380 Patent uses the term[] "application packet" . . . to refer to . . . the [protocol data unit] associated with the referenced level."); Pl.'s Suppl. Br. at 5, ECF No. 445 ("As used in the context of the '380 Patent, a POSITA would understand an 'application packet' as a packet that contains application data and an 'application layer packet' as a packet at the application layer of a networking model.").

[14] Some instances of the relevant terms can be found as follows: application packets, '380 Patent at 13:52; IP packets, *id.* at 2:43–44; "IP packets containing one or more TCP packets," *id.* at 6:1–2; "application-level HTTP packet," *id.* at 2:44–45; "TCP packets," *id.* at 6:29; and "encrypted packets," '573 Patent at 15:33.

the ’797 Patent references different layers related to corresponding packets. *See* ’797 Patent at 4:30–64 (“Each of entries 306, 308, and 310 may include data associated with their respective corresponding packet, including for example, network-layer information . . . , transport-layer information . . . , application-layer information . . . .”). Even without endeavoring to differentiate or define these different types of packets, it is evident from the claim language that the term “packet” is used in a variety of contexts and ways. This supports adopting the plain and ordinary meaning of the term in the contexts in which it appears.

The extrinsic evidence cited by both parties supports this interpretation. For example, Defendant cites Newton’s Telecom Dictionary which defines the term as a “[g]eneric term for a bundle of data” which may be termed by the “specific native protocol” as a “packet, block, frame or cell.” Harry Newton, *Newton’s Telecom Dictionary* 588 (19th ed. 2003), ECF No. 358-23.; *see also* John C. Rigdon, *Dictionary of Computer and Internet Terms* 354 (1st ed. Aug. 2016), ECF No. 364-4 (defining packet to have four different meanings including both an “(OSI) network layer transmission unit” and a “unit of information transmitted from one computer or device to another on a network”).

Similarly, Plaintiff cites to extrinsic evidence explaining that packets are generally “a small segment of a larger message” that is transmitted over computer networks. *What is a Packet? Network Packet Definition*, Cloudflare, https://www.cloudflare.com/learning/network-layer/what-is-a-packet/, ECF No. 446-2. However, packets “are sometimes defined by the protocol they are using,” for example, a packet at the network layer “can be referred to as an ‘IP packet.’” *Id.*; *see also OSI Model*, TheNetwork Seal, https://thenetworkseal.wordpress.com/stp/network/, ECF No. 360-18 (referencing OSI model which notes that “packets” are dealt with at the network layer); Goodrich Decl. ¶ 21, ECF 361 (listing “handshake packets” as a type of packet that “are usually exchanged at the beginning of a communication session"); Meriem Ferdjouni, *Cases Where Data Packet Has an Empty Payload*, Medium (Feb. 24, 2021), https://ferdjounim.medium.com/cases-where-data-packet-has-an-empty-payload-fddfea9affb5, ECF No. 360-19 (describing types of packets that are "not for the purpose of transmitting data" such as an "[a]cknowledgment" signal, a "[n]egative [a]cknowledgment [s]ignal," and an "ACKed [u]nseen [s]egment").

For these reasons, similar to those previously articulated by the Court, the Court finds that this dispute is best resolved by adopting the plain and ordinary meaning of the term in the context which it appears.

Court's Construction
Plain and ordinary meaning in the context of the claim in which the term appears

G. "A plurality of packet security gateways that collectively provide an entire interface across a boundary of a network"

The term "a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network" appears in claim 8 of the '437 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
Plain and ordinary meaning	"two or more packet security gateways arranged such that there is no network path across a boundary of a network that bypasses the packet security gateways"

The crux of this issue is what it means for the packet security gateways to provide an "entire interface" across a network boundary. PAN argues that the "'plurality of packet security gateways' must be arranged such that there is no network path across *that boundary* that bypasses the packet security gateways." Def.'s Resp. Br. at 6, ECF No. 363 (emphasis added). Centripetal argues that

PAN's construction is not supported by the intrinsic evidence or a clear disavowal of claim scope and would read out embodiments described in the specification. Pl.'s Opening Br. at 26, ECF No. 359; Pl.'s Resp. Br. at 20, ECF No. 366. The Court disagrees with Centripetal. The claim language, embodiments, and Centripetal's statements to the PTAB support PAN's proposed construction.

Here the claim language is highly instructive. Claim 8 of the '437 Patent provides that when executed, the instructions cause the system to:

> provision a packet security gateway, of *a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway* and one or more networks other than the network protected by the packet security gateway, with one or more packet filtering rules *to be applied to all network traffic* traversing the boundary, wherein each packet filtering rule comprises at least one packet matching criterion associated with malicious network traffic and a corresponding packet transformation function.

'437 Patent at 22:27–39 (emphasis added). From the claim language it is apparent that the packet security gateways are arranged in such a way that they fully protect a boundary between the protected network and another network, and that all network traffic flowing from the other network to the protected network must pass through a packet security gateway and be subject to packet filtering rules. However, the language does not foreclose the possibility of a boundary with a third network that remains unprotected.

This understanding is confirmed by Figure 8 in the specification:

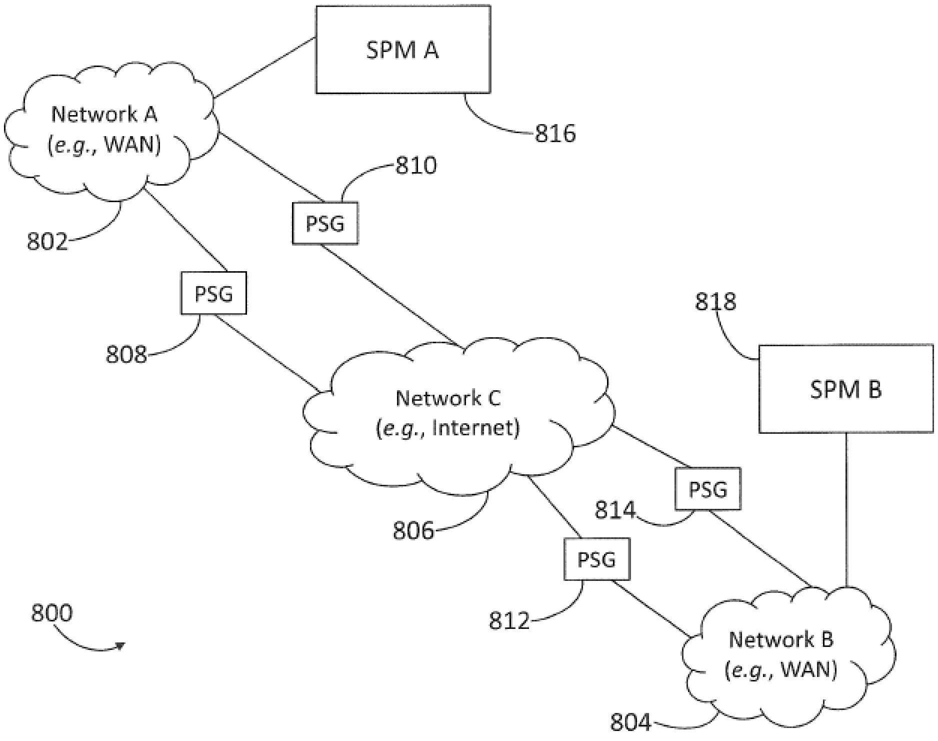

FIG. 8

Id. at fig. 8. This example shows two boundaries fully protected by a plurality of packet security gateways—the first between Network A and Network C, and the second between Network B and Network C. However, the boundary between Network A and Network B and their corresponding Security Policy Managers (SPM A and SPM B) is unprotected. Contrary to Centripetal's contention, PAN's proposed construction encompasses this example. The proposed construction states: "Two or more packet security gateways arranged such that there is no network path across *a boundary* of a network that bypasses the packet security gateways." Def.'s Resp. Br. at 5, ECF No. 363 (emphasis added). Read with the rest of the claim language, the construction does not state that the boundary between the secured network and all other networks must be protected, but instead if *a boundary* between two networks is protected, there may be no unprotected network path across *that boundary*.

This understanding is confirmed by Centripetal's statements in IPR proceedings before the PTAB. *See Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01154, Paper 7, Patent Owner's Prelim. Resp., at 34–45, 55, 63 (P.T.A.B. Oct. 25, 2021), ECF No. 358-3; *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01153, Paper 7, Patent Owner's Prelim. Resp., at 32–43, 56, 60 (P.T.A.B. Oct. 25, 2021), ECF No. 358-4. In its arguments before the PTAB, Centripetal stated the preamble should be treated as limiting. *See Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01154, Paper 7, Patent Owner's Prelim. Resp., at 34–45, 55–56 (P.T.A.B. Oct. 25, 2021), ECF No. 358-3 ("The preambles also recite the 'plurality of packet security gateways that collectively provide an entire interface across a boundary of a [protected] network,' which is 'essential to understand' the 'all traffic' limitation in the body of these claims and thus 'give life, meaning, and vitality' to the claims." (internal citations omitted)). Further, when distinguishing against the prior art, Centripetal argued that the prior art did not disclose the "entire interface" limitation because the prior art allowed "network paths across the alleged 'boundary'" that bypassed the security barrier, i.e. edge servers. *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01153, Paper 7, Patent Owner's Prelim. Resp. at 32 (P.T.A.B. Oct. 25, 2021), ECF No. 358-4 (" . . . *Jungck* describes network paths across the alleged 'boundary' that bypass *Jungck's* edge servers, demonstrating that the edge servers do not form the 'entire interface' across the alleged boundary."). This confirms the understanding that if the boundary between two networks is protected, then all network traffic between the two networks must be filtered through the packet security gateways.

For these reasons, the Court adopts PAN's proposed construction.

Court's Construction
"two or more packet security gateways arranged such that there is no network path across a boundary of a network that bypasses the packet security gateways"

H. "Provision a packet security gateway . . . with one or more packet filtering rules"

The term "provision a packet security gateway . . . with one or more packet filtering rules" appears in the claim 8 of the '437 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
Plain and ordinary meaning	"communicating one or more packet filtering rules to a packet security gateway"

The dispute in this construction centers around whether "provision" is limited to "communicating" the packet filtering rules to the packet security gateway. Centripetal concedes that "[s]ome embodiments involve instances where the system's security policy management server can communicate rules to the packet security gateway." Pl.'s Opening Br. at 17, ECF No. 359. However, Centripetal argues that the packet security gateway may also be "provisioned" by receiving a policy information update, something that it claims would be foreclosed if the Court adopted PAN's proposed construction. *Id.* at 17–19. The Court agrees with Centripetal.

Claim 8 of the '437 Patent provides that when executed, the instructions "cause the system to: *provision a packet security gateway . . . with one or more packet filtering rules* to be applied to all network traffic traversing the boundary." '437 Patent at 22:29–36 (emphasis added). While this claim itself does not shed light on the term "provision," a dependent claim, claim 14, supports Centripetal's position. Claim 14 describes the packet security gateway receiving a policy information update and then, based on that update, the packet security gateway creates or alters the filtering rules. *See id.* at 23:57–67 ("[R]eceiving, by the packet security gateway, a *policy* *information update*; and at least one of *create or alter*, based on the policy information update . . . , at least one packet matching criterion associated with malicious network traffic and a packet transformation function of *one or more packet filtering rules*." (emphasis added)). In this dependent claim, the rules are not being communicated to the packet security gateway but instead the packet security gateway receives a policy information update which then either creates or alters the rules. PAN's proposed construction is inconsistent with this dependent claim.[15] Accordingly, the Court rejects PAN's proposed construction. *See Wright Med. Tech., Inc. v. Osteonics Corp.*, 122 F.3d 1440, 1445 (Fed. Cir. 1997) (explaining that the Court "must not interpret an independent claim in a way that is inconsistent with a claim which depends from it").

For the reasons stated above, the Court adopts the plain and ordinary meaning of the term.

Court's Construction
Plain and ordinary meaning

I. "Rule(s)"

The term "rule(s)" appears in claim 8 of the '437 Patent, claims 16 and 25 of the '380 Patent, claims 1 and 9 of the '573 Patent, and claims 1, 12, and 17 of the '797 Patent. The parties have proposed the following constructions:

Centripetal's Construction	PAN's Construction
"a condition or set of conditions that when satisfied cause a specific function to occur"	"an identification of a condition or set of conditions and the specific function(s) to perform when met"

[15] PAN also argues that the PTAB proceedings for U.S. Patent No. 9,560,077, the grandparent patent of the '437 Patent, support its proposed construction. Def.'s Opening Br. at 9–10, ECF No. 357. However, the Court does not find the PTAB's construction probative because that construction dispute centered on whether "provisioning" was broad enough to encompass "changing a device from one state to another" not whether "provisioning" should be limited solely to "communicating." *See Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2018-01513, Paper 7, Institution Decision at 7–8 (P.T.A.B. Apr. 2, 2019), ECF No. 358-7.

The parties agree that "rule(s)" should be construed consistently across all asserted claims. Def.'s Opening Br. at 10, ECF No. 357; Pl.'s Opening Br. at 13, ECF No. 359. The construction proposed by Centripetal was adopted by this Court in previous litigation involving patents from similar patent families[16] as the patents asserted here. *See Centripetal Networks, Inc. v. Keysight Techs., Inc.*, No. 2:17-cv-00383, ECF No. 484 (E.D. Va. Sept. 11, 2018). PAN argues that its proposed construction is necessary to clarify that "rules" must contain both a condition and the related function to be performed. Def.'s Opening Br. at 13, ECF No. 357. Centripetal argues that this construction does not make sense when applied to certain embodiments and is inconsistent with the '437 Patent's specification. *See* Pl.'s Resp. Br. at 10–11, ECF No. 366. The Court agrees with Centripetal's construction.

As discussed above, Claim 8 of the '437 Patent provides that when executed, the instructions "cause the system to: *provision a packet security gateway* . . . *with one or more packet filtering rules* to be applied to all network traffic traversing the boundary." '437 Patent at 22:27–36 (emphasis added). This can occur by a packet security gateway receiving a policy information update that creates or alters the packet filtering rules. *Id.* at 23:57–67; *see also supra* Part II.H. As the specification explains, this can include "rules that specify a list of network addresses known to be associated with malicious network traffic." *Id.* at 14:12–14. In that situation, the newly provisioned rules may contain an updated list of malicious IP addresses (conditions) but do not contain a corresponding update to the function (i.e. to block the IP address). *See id.* at 14:6–36. Construing "rule(s)" as always containing both the condition and function would read out this embodiment where the "provisioned rules" are merely a list of updated conditions.

[16] The patents at issue in *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, included U.S. Patent No. 9,264,370 from the Ahn family of patents and U.S. Patent No. 9,137,205 and U.S. Patent No. 9,560,077 from the Rogers family of patents, among others.

Centripetal's proposed construction—"a condition or set of conditions that when satisfied cause a specific function to occur"—retains both the "if/then" function of rules, *see* Goodrich Decl. ¶ 24, ECF No. 361, while still encompassing the example discussed above. Accordingly, the Court adopts Centripetal's proposed construction.

Court's Construction
"a condition or set of conditions that when satisfied cause a specific function to occur"

III. CONCLUSION

For the reasons discussed, the Court adopts the constructions set forth above as the constructions of the ten disputed claim terms in the Asserted Patents.

It is SO ORDERED.

/s/
Elizabeth W. Hanes
United States District Judge

Norfolk, Virginia
Date: October 11, 2023